

UNCLASSIFIED

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION



J-6

DISTRIBUTION: A, B, C

CJCSI 6285.01D

21 August 2017

MISSION PARTNER ENVIRONMENT INFORMATION SHARING REQUIREMENTS MANAGEMENT PROCESS

References: See Enclosure G for References

1. Purpose. This instruction establishes the process for collecting, validating, prioritizing, and overseeing implementation of current Combatant Command's (CCMD) Mission Partner Environment (MPE) operational systems requirements as directed by reference a. The management process described in this instruction serves as a single point of entry for requirements to support modernization, enhancements, and system development efforts for existing programs within the Defense Information System Agency's (DISA) Multinational Information Sharing (MNIS) portfolio. Additionally, these requirements may be used to inform future doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy development and other joint requirements generation processes. New capabilities will be assessed for operational validation and passed to the appropriate organization for sponsorship through the Joint Capabilities Integration and Development System (JCIDS) process. Request for network connections will be in accordance with references p, q, and r and not applicable to this process. Existing MPE information sharing systems and services covered by this instruction are listed in Enclosure D. U.S. Battlefield Information, Collection, and Exploitation Systems (US BICES) and U.S. BICES eXtended (US BICES-X) requirements are addressed in paragraph 4.e. Joint command and control (C2) requirements will follow the procedures outlined in reference k. The MPE requirements management process will evolve over time to keep pace with warfighter needs and technological improvements, and remain aligned to the MPE governance and management processes outlined in reference a and b.

2. Superseded/Cancellation. CJCSI 6285.01C, "Multinational and Other Mission Partner (MNMP) Information Sharing Requirements Management Process," 15 May 2013, is hereby superseded.

UNCLASSIFIED

21 August 2017

3. Applicability. This instruction applies to Joint Staff (JS), CCMDs, Services, Defense Agencies, and mission partners.

4. Guidance

a. The process defined in this instruction integrates CCMDs' MPE requirements and priorities across all phases of military operations (Shape the Environment, Deter the Enemy, Seize the Initiative, Dominate the Enemy, Stabilize the Environment, Enable Civil authority). MPE requirements will be submitted as Capability Needs (CNs) by CCMDs at any time via the Joint Staff J-6 Net-Enabled Requirements Identification Database (NRID) on SIPRNET <<http://intelshare.intelink.sgov.gov/sites/nrid>> or NRID-U on NIPRNET <<https://intelshare.intelink.gov/sites/ccd/ds/NRID-U/SitePages/Home.aspx>> per the procedures in the NRID Quick-Help guide found on the website. CNs for new capabilities that are outside of the DISA MPE information sharing systems portfolio are not considered suitable for this process and will be assessed for potential submission via the JCIDS process or the C2 Governance and Management process (see Enclosure B). The JS J-8-sponsored Knowledge Management and Decision Support System will continue to be used to manage JCIDS documents for Joint Requirements Oversight Council (JROC) validated capabilities and requirements.

b. The ability to share classified and unclassified information with mission partners is a critical element in multinational operations. The DISA MNIS office managed Combined Enterprise Regional Information Exchange System (CENTRIXS), Pegasus, Releasable Demilitarized Zone (REL/DMZ), Common Mission Network Transport (CMNT), Combined Federated Battle Laboratories Network (CFBLNet), Unclassified Information Sharing Service (UISS) – All Partners Access Network (APAN), CENTRIXS modernization aligned with the Mission Partner Environment-Information System (MPE-IS) reference architecture, Cross Domain Enterprise Services (CDES), and supporting infrastructure and services provides the environment to enable multinational operations. These operational and direct support networks/information systems may be included in Department of Defense (DoD) efforts to improve mission partner information sharing and effectiveness.

c. CCMDs will submit all MPE requirements through the JS submission process as CNs with an O-6 endorsement from their organization. CCMDs are encouraged to review the checklist in Enclosure E prior to submission of a CN. Mission critical requirements falling outside of the annual cycle will be accepted for immediate adjudication and validation through the out-of-cycle process outlined in Enclosure B (Figure 2).

21 August 2017

d. Service, Agency, and mission partner information sharing CNs must be sponsored and submitted by a CCMD or the Joint Staff acting on behalf of multiple CCMDs.

e. Capabilities and services applicable to this instruction are listed in enclosure D. US BICES and US BICES-X, as the designated DoD Coalition Intelligence Information Sharing enduring capability and the intelligence component of the DoD Mission Partner Environment; however, these two programs are outside the DISA MNIS portfolio. US BICES and BICES-X requirements management and oversight is provided by the Defense Intelligence Information Enterprise (DI2E) Council. CCMDs CNs submitted that are assessed to be solely US BICES and BICES-X requirements will be forwarded to the DI2E Council for consideration. The submitting CCMD will be notified when this occurs. The JS J-6 will consolidate and forward these CNs for consideration by the DI2E Council through the Intelligence Community Capability Requirements process.

f. The DISA CENTRIXS modernization effort is aligned to the MPE-IS reference architecture. At the time of publishing, DISA has a limited MPE-IS "in service" capability to support CCMD MPE mission enclave requirements. Until a storefront process is established, CCMDs will be required to submit CNs, using the processes outlined in this instruction, to establish a mission enclave hosted by DISA's MPE services.

g. MPE requirements that were prioritized for resourcing but remain unfunded are considered valid requirements and will be reviewed annually for accuracy and prioritization.

h. Solutions for validated and unfunded MPE requirements that will be funded by an appropriate organization and implemented by DISA will be aligned, as appropriate, to the MPE-IS reference architecture and require an agreed upon transition plan capturing the implementation and sustainment funding responsibilities until transitioned to the DISA Program Objective Memorandum or a Program Decision Memorandum.

i. Funded MPE requirements that require an update or modification to clarify the requirement due to technology improvements or enhancements that are within the scope of the original requirement submission and within the sustainment baseline for the requirement will be addressed through a letter of clarification (LOC). The LOC will require an O-6-level endorsement from their organization prior to submission to the JS J-6 for approval. See Enclosure F for an example letter of clarification.

21 August 2017

j. Department of Defense Information Network (DODIN) connections to support MPE mission enclaves will be processed in accordance with references p, q, and r and do not require a CN/NRID submission.

k. Once an MPE requirement solution has transitioned into the DISA storefront/service catalog, a CN/NRID submission is not required.

1. The following mission impact criteria will be used when submitting MPE information sharing CNs:

(1) Mission Critical. Prevents accomplishment of mission critical capability with direct impact on mission failure and/or readiness; no work-around or alternative exists. Capability is needed immediately to mitigate risk.

(2) Mission Essential. Adversely affects the accomplishment of, or degrades, a mission essential capability and no acceptable work around or alternative solutions exist; requirement is needed to maintain sufficient military capability and is needed no later than a specific date to prevent the loss/degradation of capability.

(3) Mission Improvement. Adversely affects accomplishment of, or degrades, mission essential capability and work-around / alternative solution is known; improvement will provide increase in mission capability.

(4) Mission Enhancement. Addresses enhancements not critical or essential for mission accomplishment; increases efficiency, addresses user/operator annoyance with system functions beyond a help desk or problem report to resolve.

m. The Command, Control, Communications, and Computers (C4)/Cyber Functional Capabilities Board (C4/Cyber FCB), in coordination with other relevant Capability Boards (e.g. Battlespace Awareness, Logistics, Force Application, Force Protection), will assess MPE requirements against competing priorities, available resources, and constraints to approve requirements for implementation.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes. Redefined scope of instruction. Ensured all DoDI 8110.1 guidance, authorities, and responsibilities for the Joint Staff were adequately addressed. Updated timelines, categorization, priorities, process flow, and responsibilities for MPE requirement management process. Added letter of clarification processes. Updated MPE requirements management

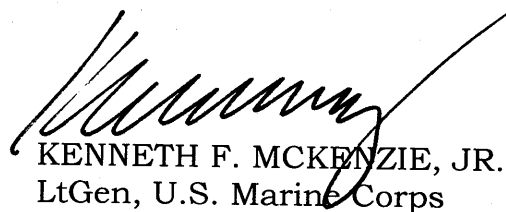
21 August 2017

process flow chart Figure 1 and Figure 2. Updated responsibilities in Enclosure A. Removed requirement to submit a CN/NRID to establish a network connection to an existing network and for services provided through a service catalog. Removed Services and Agencies from submitting CNs.

8. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on NIPRNet. DoD Components (to include the CCMDs), other Federal agencies, and the public, may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at: <http://www.dtic.mil/cjcs_directives/>. JS activities may also obtain access via the SIPR Directives Electronic Library Websites.

9. Effective Date. This INSTRUCTION is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:



KENNETH F. MCKENZIE, JR.
LtGen, U.S. Marine Corps
Director, Joint Staff

ENCLOSURES:

- A - RESPONSIBILITIES
- B - MPE INFORMATION SHARING REQUIREMENTS MANAGEMENT
PROCESS FLOW CHART
- C - MPE REQUIREMENTS REQUEST FORMAT TEMPLATE
- D - EXISTING MPE INFORMATION SHARING SYSTEMS AND SERVICES
- E - MATRIX / CHECKLIST OF AGREEMENTS, AUTHORITIES, POLICIES
- F - SAMPLE LETTER OF CLARIFICATION
- G - REFERENCES
- GL- GLOSSARY

INTENTIONALLY BLANK

ENCLOSURE A

RESPONSIBILITIES

1. The Chairman of the Joint Chiefs of Staff (CJCS) serves as the primary focal point for collecting, adjudicating, prioritizing, and validating MPE information sharing requirements and providing them to the appropriate organization for proper planning, engineering, and execution. All MPE information sharing requirements will be addressed utilizing the appropriate process flow chart located in Enclosure B. The process will ensure interoperability, integration, compatibility, prioritization, and consistency of requirements across requesting CCMDs.

a. The JS J-6 will:

(1) Provide oversight of the entire MPE (classified and unclassified) requirements management process.

(2) Consolidate CCMD requirements annually to capture new CNs and to revalidate and prioritize previously approved but unfunded MPE information sharing requirements for implementation determination.

(3) Review and process out-of-cycle mission critical CNs that must be met prior to the next annual requirements consolidation and prioritization process cycle as outlined in Figure 2 of Enclosure B.

(4) Determine and assign a requirements sponsor (support/lead) organization, as needed. CCMDs and the JS J-6 may sponsor requirements for capabilities that span multiple CCMDs.

(5) Review CN submissions for completeness and clarity, conduct meetings with appropriate stakeholders to verify content of submissions, ensure they fit into the DISA MNIS information sharing systems and services portfolio, and determine suitability for continued processing. Acceptable requirements must meet policy, security, and regulatory guidelines.

(6) Consolidate and forward MPE requirements to the JS J-3 for validation and prioritization.

(7) Coordinate the JS J-3 MPE requirements prioritization results with the CCMDs. For those requirements not validated return to the CCMD for resubmittal or closure.

(8) Present the JS J-3 prioritized MPE requirements to the C4 Cyber FCB Chair for endorsement and forward to DISA for technical and resource strategy development.

21 August 2017

(9) Coordinate recommended resource strategy—to include roles and responsibilities, technical solution, implementation plan/schedule and cost estimates—with requirements sponsor and DISA.

(10) Assist DISA in making preparations to present final resourcing strategy—to include roles and responsibilities, technical solution, implementation plan/schedule, cost estimates, and recommended funding strategy—to the C4/Cyber FCB or appropriate FCB for approval. Provide final results to the requirement sponsor.

(11) Facilitate and endorse out-of-cycle mission critical requirements whose resource strategies, costs, and implementation plan will not delay or defer DISA efforts to meet current requirements. Forward out-of-cycle mission critical requirements that will delay or defer DISA efforts to implement existing C4/Cyber FCB approved requirements to the JS J-3 for prioritization and C4/Cyber FCB for approval.

(12) Coordinate and process letter of clarification submission.

(13) Maintain MPE information sharing requirements in the NRID databases with the current status of the requirement.

b. The JS J-3 will:

(1) Validate and prioritize MPE information sharing requirements and forward to the JS J-6 for further processing.

(2) Validate and prioritize out-of-cycle requirements based on approved/ongoing requirements and forward to the JS J-6 for further processing.

c. C4/Cyber FCB will:

(1) Provide oversight and final decision authority for MPE requirements evaluation, advocacy, and support for CCMDs, Services, and Agencies.

(2) As required, coordinate and align MPE requirements with other Capability Boards.

(3) Endorse JS J-3 validated and prioritized requirements for resource analysis and, upon receiving the DISA resource plan, approve MPE requirements and prioritization for implementation.

d. DISA will:

21 August 2017

(1) Develop plans, programs, and budgets for MPE capabilities and supporting infrastructure and infrastructure services to satisfy both current and unfunded requirements, to include the migration of operational system capabilities to an enterprise level aligned to the MPE-IS reference architecture.

(2) Upon the C4 Cyber FCB Chair endorsement of MPE requirements, coordinate directly with the appropriate stakeholders and provide a recommended resourcing strategy, which includes technical solutions, SME support, implementation plan/schedule, costs, and requirements that can be met with existing resources to the JS J-6 for staffing.

(3) Based on CCMD, Service, and Agency funding input, update final recommended resourcing strategy to include appropriate support agreements.

(4) Upon C4/Cyber FCB approval of MNIS requirements and prioritization, execute the implementation plan. As required, provide updates to the JS J-6 on the implementation status.

(5) Ensure MNIS information sharing requirements solutions are appropriately aligned with current DODIN operations policies and, as appropriate, the DI2E policies. Solutions, as appropriate, will be aligned to the MPE-IS reference architecture. In coordination with JS J-6, determine where migration of DISA's MNIS information sharing systems and services to an enterprise service level and implement that migration within programmed funding constraints.

(6) Maintain and publish a MPE information sharing service catalog, and the Defense Information Systems Network (DISN) connection process guide to support the "in service" capabilities. Update the information sharing service catalog annually.

e. Combatant Commands will:

(1) Submit CNs to the JS J-6 through the process outlined in this instruction. If the submitter is unable to access NRID, the CN may alternatively be submitted via email using the format and all criteria as identified in Enclosure C.

(2) Develop policy and procedures applicable to your command for sponsorship of Service Component, Defense Agency, or mission partner MPE requirements.

(3) Revalidate unfunded requirements for applicability, accuracy, and priority order during each annual MPE requirements management process cycle.

21 August 2017

(4) For unfunded requirements, review the recommended technical solutions, costing, and implementation schedules and determine if another appropriate organization has agreed to fund this requirement or defer the requirement. Provide your response to the JS J-6.

(5) Coordinate funding with appropriate organization to fund user-level requirements, to include, but not limited to: workstations or terminals, software licensing requirements, and cybersecurity requirements, as well as the supporting network transport infrastructure from the DISN/DODIN/CMNT Point of Presence to the Customer Edge (CE) and beyond.

(6) Comply with all references, related processes, publications, and policies listed in Enclosure E when submitting requirements.

f. Services, Agencies, and Mission Partners will provide support to this process and may be assigned duties as the requirement sponsor by the C4/Cyber FCB.

ENCLOSURE B

MPE INFORMATION SHARING REQUIREMENTS MANAGEMENT PROCESS

1. Purpose. Providing timely, detailed, well-understood, and actionable requirements to the materiel development community is critical to putting the right capability into the hands of warfighters. This section outlines the processes for identifying, capturing, processing, and prioritizing requirements and implementing solutions into existing MPE systems/services outlined in Enclosure D. See Figure 1 for routine MPE information sharing requirements management process flow chart and Figure 2 for out-of-cycle MPE information sharing requirements management process flow chart.

2. Identify/Submit. During this phase the user identifies new capability needs and obtains O-6-level endorsement from their organization prior to submission of the CN into NRID. CCMD users need to ensure their NRID submissions reflect MPE operational requirements for systems and services identified in Enclosure D. NRID will not be used to submit Problem Reports for service/help desk related problems, change request for enterprise services, and letter of clarifications for approved and funded requirements.

3. Verify/Assess. During this phase the JS J-6 reviews the CN with subject matter experts (SMEs) to determine if the requirement is suitable for processing via the MPE information sharing requirements management process. Once the CN is clearly understood and deemed suitable the CN moves to the assessment portion of the Verify/Assess phase. As required, SMEs will meet to assess the CN for acceptability using the following criteria:

a. Suitable. The CN constitutes an extension of, or improvement to, an existing requirement or enhancement to a system or service outlined in Enclosure D.

b. Unsuitable. Requests for new capabilities not currently in the portfolio of systems listed in Enclosure D to this instruction. For requests of new capabilities that are unsuitable for processing within the MPE information sharing requirements management process, the JS J6 will notify the sponsoring CCMD whether the requirement was transferred to an appropriate process or not found suitable for further processing.

c. Acceptable. Suitable requirements are assessed for acceptability by the JS J-6 and, as required, SMEs. A CN is considered acceptable if it meets security, regulatory, and policy standards. The JS J-6 will ensure acceptable CNs are aligned with the Joint Information Environment (JIE) objectives before further processing. The JS J-6 may use functional area working groups (e.g. MPE Executive Steering Committee Requirements and Capabilities Development Working Group) to assess acceptability. When found acceptable,

21 August 2017

the JS J-6 will develop a recommended prioritization order for the JS J-3 to use for validation and prioritization. The JS J-6 will notify the CCMD when a CN was found not acceptable for this process.

4. Prioritization. During this phase the JS J-6 will forward the accepted CNs to the JS J-3 for validation and prioritization. Upon completion of the JS J-3 prioritization, the requirements will be coordinated with the CCMD and forwarded to the C4 Cyber FCB for approval. Upon endorsement, the C4 Cyber FCB will request DISA to provide a resourcing strategy for the prioritized requirements and present this strategy to the C4/Cyber FCB to support a cost informed decision for the prioritized requirements. The prioritization phase will conclude when the C4 Cyber FCB Chair endorses the JS J-3 validated and prioritized MPE requirements.

5. Solution. During this phase DISA will coordinate with the appropriate stakeholders to develop the technical solution and resourcing strategy. As applicable, solutions will be aligned to the MPE-IS reference architecture. Upon completion, the JS J-6 and DISA will provide the validated MPE requirements and recommended resourcing strategy to the C4/Cyber FCB or appropriate FCB for review and approval. Upon approval, the C4/Cyber FCB or appropriate FCB will forward the approved prioritized requirements to DISA for implementation. DISA will coordinate with the requirement sponsor for implementation and incorporation into the DISA MPE sustainment baseline and service catalog. Those requirements that were not resourced will be considered valid requirements but unfunded, unless the requirement sponsor or appropriate organization funds for the implementation and sustainment of the approved resource strategy. The requirement will remain open in the NRID database until the CCMD confirms the solution has satisfied the requirement.

ROUTINE MPE INFORMATION SHARING REQUIREMENTS MANAGEMENT PROCESS FLOW CHART

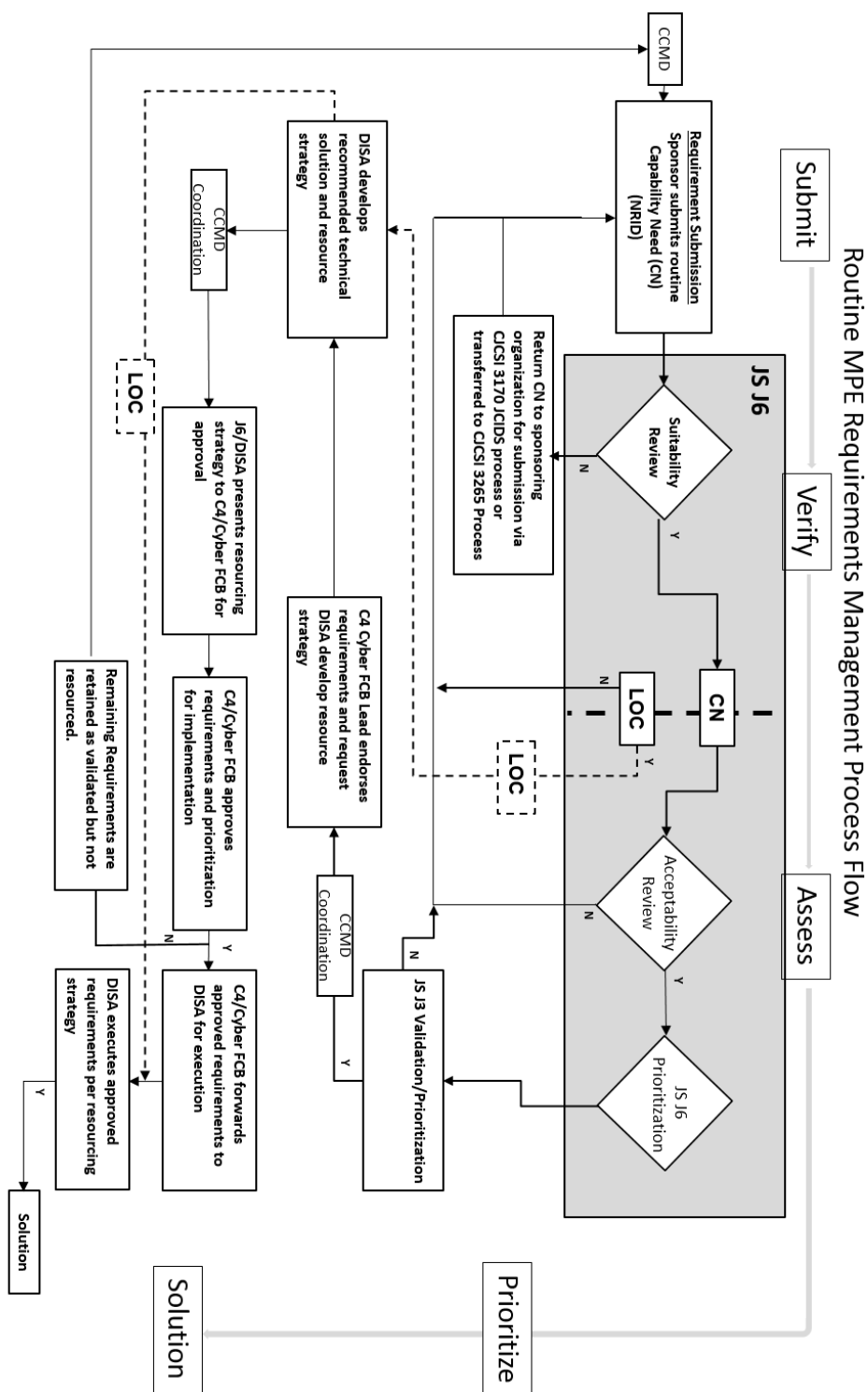


Figure 1: Routine MPE Information Sharing Requirements Management Process Flow Chart

OUT-OF-CYCLE MPE INFORMATION SHARING REQUIREMENTS MANAGEMENT PROCESS FLOW CHART

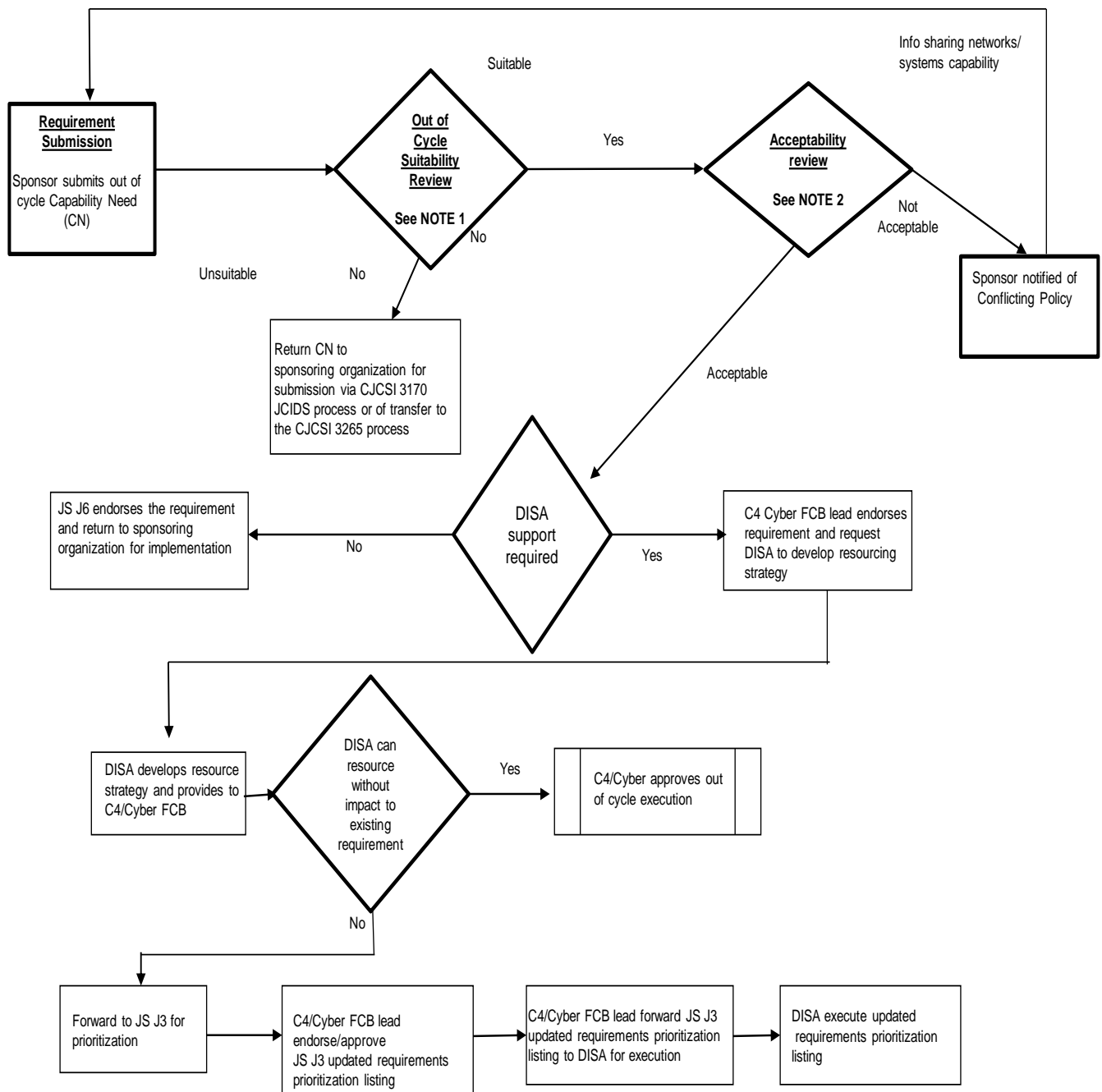


Figure 2. Out-of-Cycle MPE Information Sharing Requirements Management Process Flow Chart

Figure 2 Notes

Note 1: JS J-6 will assess all Mission Critical out-of-cycle requirement for suitability and acceptability. Mission Critical out-of-cycle requirements assessed as not suitable will be returned to the sponsor with a letter of unsuitability from the JS J-6. The unsuitable mission critical out-of-cycle requirement may be processed via the semi-annual requirements process, for submission via CJCSI 3170 JCIDS process, or the C2 Governance and Management process in accordance with reference k and l.

Note 2: Mission Critical out-of-cycle requirements will be assessed against the same acceptability criteria defined for in-cycle requirements found in paragraph 3.c. above. Requirements that align with the DISA MPE portfolio will be forwarded to DISA for support.

INTENTIONALLY BLANK

ENCLOSURE C

MPE INFORMATION SHARING REQUIREMENTS
REQUEST FORMAT TEMPLATE1. MPE Information Sharing Requirements Capability Need Request

a. Mission Impact (Mission Critical, Mission Essential, Mission Improvement, Mission Enhancement).

b. Operational Requirement. State the operational requirement and capability (e.g., Require a radio gateway connection to CENTRIXS-X that provides an interconnection between various sets of radio networks allowing secure, tactical, real-time, high fidelity video, data, and voice services to be deployed in a networked environment to support tactical operations). **Do not identify solutions.**

c. Capability Need Description. Detailed description of operational capabilities; operational gaps/shortfall requirement will address; and mission criticality (critical, essential, improvement, enhancement). Link operational shortfall to Joint Urgent Operational Needs Statement, Operational Needs Statement, and/or Initial Capability Document. Examples of operational gaps/shortfalls include:

(1) nonexistent or limited use of C2 services in a Disconnected Intermittent or Limited bandwidth environment.

(2) limited ability to maintain and share situational awareness (SA) while On The Move (OTM).

(3) lack of ability for leaders to provide accurate and timely guidance and intent of Coalition Forces and Afghan National Security Forces mission partners while OTM.

(4) inability to collaborate OTM.

d. Threshold and objectives. As appropriate, provide Service-level requirements and/or key performance indicators to support the operational requirement. For example, desired availability, expected utilization rates, etc.

e. Justification

(1) Impact to mission if requirement not met.

(2) Expected benefits.

(3) Workarounds in place.

f. Operational Endorsement. Attach a separate memorandum signed by appropriate sponsor (0-6 endorsement).

g. Submitter's Contact Information

h. Submitter's Supervisor Contact Information

i. Requirement Point of Contact Information (applicable stakeholders)

j. Type of capability. New capability; sustainment of, extension of, or improvement to an existing capability.

k. Interoperability. Fully interoperable and compatible with current as well as future international standards, (e.g., IPV6) and legacy systems currently in use (e.g., CENTRIXS family of systems).

l. Service/Agency-Managed Systems the solution must be compatible with (e.g., Theater Battle Management Core System, or Battle Command Common Services).

m. Responsibility for Requirement Costs (e.g., design, implementation and sustainment): (Customer, DISA, N/A).

n. Training Requirements

o. Additional Human Resources Required

p. Logistics Support (e.g., CJCSI 6510.06 Series, "Communications Security Releases to Foreign Countries")

q. Capability Categorization. Command and Control mission application; Information Sharing Network/system.

r. CCMD/Service/Agency Priority: (e.g., #1 of 5)

s. Brief History of Previous Submissions

t. Additional Comments

ENCLOSURE D

EXISTING MPE INFORMATION SHARING SYSTEMS AND SERVICES

1. SIPRNET REL DMZ: Defined as all U.S. SIPRNET enclaves extended to enable Five Eyes (FVEY) partner access to Secret-Releasable information.
2. Common Mission Network Transport. See glossary for definition.
3. Combined Enterprise Regional Information Exchange System. See glossary for definition.
4. Pegasus. See glossary for definition.
5. Combined Federated Battle Laboratory Network. Provides the infrastructure for international/multinational (Combined Communications Electronics Board (CCEB), NATO, United States, and approved Mission Partners) Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) research, development, trials and assessment to support coalition interoperability with member Nations.
6. Unclassified Information Sharing Services. The UISS enterprise solution provides unclassified collaboration and information sharing for U.S. DoD and mission partners participating in joint/combined operations, humanitarian assistance and disaster recovery operations, and international conferences or other collaboration events. UISS provides compatible open source software, Commercial Off-the-Shelf Software, and government unique software (e.g., APAN).
7. Cross Domain Enterprise Services. Provides support to CCMDs, Services, and agencies by implementing, fielding, and providing lifecycle support for cross domain solution technologies. DISA provides consolidated cross domain solutions on behalf of the DoD components and develops a robust cross domain fielding capability under reference s.
8. Mission Partner Environment-Information System. MPE-IS is the U.S. portion to MPE and is the DISA-managed modernization effort in development and not planned to be completed until fiscal year 2022. At the time of publication, a limited capability will be available to support CCMD MPE information sharing requirements. MPE-IS will be enabled by DISA Information Technology (IT) infrastructure that includes networks, cybersecurity, data centers, cross domain solutions, and user interfaces. The CCMD Components are responsible for B/P/C/S infrastructure to develop MPE-IS service for the CE to the end user. The above legacy system and services will be integrated as appropriate to support the rapid establishment of

21 August 2017

enduring and episodic mission enclaves in support of CCMD MPE information sharing requirements.

9. Virtual Data Center (VDC). VDC is a modernization of mission enclaves that supports the MPE-IS reference architecture. The VDC provides a multi-enclave virtualization system that delivers the same functions as a physical data center and can host multiple discrete mission enclaves enduring and episodic missions).

ENCLOSURE E

MATRIX/CHECKLIST OF AGREEMENTS, AUTHORITIES, POLICIES

Below is a matrix/checklist of information sharing references (agreements, authorities, and policies) that CCMDs, Services, and agencies must address prior to submitting a CN. This front-loaded guidance for users will streamline the appropriate requirements working group's efforts by arming the command with information sharing expectations from a policy, security, and operational/technical perspective.

| COUNTRY | INTERNATIONAL AGREEMENT (DoDD 5530.3) | CONPLANS/ OPORD (Command) | CISMOA (CJCSI 6510) | GISMOA (NDP-1) | TECHNICAL AGREEMENT (DoDD 5530.3) | EXCEPTIONS TO NATIONAL DISCLOSURE POLICY (NDP-1) | Foreign Military Sales/National/ Multi-Fora Agreements |
|---------|--|---------------------------------|---|---|--------------------------------------|---|--|
| X | Type of Information Exchange Agreement | XXXX-XX | Authority to transfer COMSEC hardware /software | Agreement for the protection of classified material | Country COMSEC support agreement | General information sharing specifics | Additional Agreements |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

INTENTIONALLY BLANK

ENCLOSURE F
Capability Need Letter of Clarification

COMMAND LETTER HEAD

Zip Code

Date:

MEMORANDUM FOR DEPUTY DIRECTOR, COMMAND, CONTROL,
COMMUNICATIONS, AND COMPUTERS/ CYBER,
INTEROPERABILITY DIVISION, ATTENTION: COMBINED
COALITION BRANCH

Subject: (Capability Need Title)

1. The **Subject Capability Need** requires clarification since the original validation on **Date**.
2. The capability enhancements were derived through internal **CCMD** efforts and are consistent with the Joint Staff Unclassified Sharing Service-DoD Internet Service Private (UISS-DIS Private) Capability Package.
3. The capability enhancements for clarification are:
 - a. Host select mission applications that extend the effectiveness of SOF Mission Partner collaboration (i.e., Defense Ready Strategic Engagement Application; Geospatial data information system)
 - b. View/edit Microsoft Office suite of the documents within browser.
4. This command understands that if the cost associated with this clarification are beyond the original implementation and sustainment costs, this clarification will be reprioritized through the process outlined in the CJCSI 6285.0 1D.
5. POC for this action is **Name and Phone Number**.

Name
Title

INTENTIONALLY BLANK

ENCLOSURE G

REFERENCES

- a. DoDI 8110.01, 25 November 2014, "Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD"
- b. CJCSI 5128.01 series, "Mission Partner Environment Executive Steering committee (MPE ESC) Governance and Management"
- c. CJCSI 3170.01 series, "Joint Capabilities Integration and Development System"
- d. JROCM 081-12, 31 May 2012, "Future Mission Network Initial MNIS Way Ahead"
- e. Combined Federated Battle Laboratory Network (CFBLNet) Operational Needs Statement (ONS), 27 April 2005
- f. NDP-1, National Disclosure Policy and Procedures for the Disclosure of Classified Information to Foreign Governments and International Organizations, 1 October 1988
- g. DoDI 8330.01, 21 May 2014, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)"
- h. CJCSI 6510.06 series, "Communications Security Releases to Foreign Nations"
- i. CJCSI 3265.01 series, "Command and Control Governance and Management"
- j. CJCSM 3265.01 series, "Joint Command and Control (C2) Capability Needs/Requirements Management Procedures"
- k. DoDI 8410.02, December 2008, NetOps for the Global Information Grid (GIG)
- l. DoD Directive 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"
- m. DoD Directive 5530, 11 June 1987, "International Agreements", Certified current as of 21 November 2003
- n. CJCSI 6211.02 series, "Defense Information Systems Network (DISN) Responsibilities"

- o. "Network Services Enterprise Connection Division, Defense Information Systems Network (DISN) Connection Process Guide (CPG)", Version 5.0, November 2014, <http://www.disa.smil.mil/Network-Services/Enterprise-Connections/Connection-Process-Guide.html>
- p. DISA MNIS Combined Enterprise Regional Information Exchange System Enclave Connection Approval Process (CENTRIXS ECAP), version 3.0, February 2012.
- q. DoDI 8540.01, 8 May 2015, "Cross Domain (CD) Policy"
- r. DoDI 8115.01, 10 October 2005, Information Technology Portfolio Management"
- s. Intelligence Community Directive 115, 4 December 2009, "Intelligence Community Capability Requirement (ICCR) Process"

GLOSSARY

PART I-ABBREVIATIONS AND ACRONYMS

Items marked with an asterisk () have definitions in PART II*

| | |
|-------------|---|
| APAN | All Partner Access Network |
| C4ISR | Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance |
| CCEB* | Combined Communication-Electronics Board |
| CCMD | Combatant Command |
| CDES* | Cross Domain Enterprise Services |
| CENTRIXS* | Combined Enterprise Regional Information Exchange System |
| CFBLNET* | Combined Federated Battle Laboratories Network |
| CIAV* | Coalition Interoperability Assurance and Validation |
| CISMOA | Communication Interoperability and Security Memorandum of Agreement |
| CMNT* | Common Mission Network Transport |
| CN | Capability Need |
| DISA* | Defense Information Systems Agency |
| DoD | Department of Defense |
| DODIN* | Department of Defense Information Networks |
| FCB* | Functional Capabilities Board |
| GISMOA | General Information and Security Memorandum of Agreement |
| JCIDS | Joint Capabilities Integration Development System |
| JIE* | Joint Information Environment |
| JROC | Joint Requirements Oversight Council |
| LOC | Letter of Clarification |
| MNIS | Multinational Information Sharing |
| MPE* | Mission Partner Environment |
| MPE-IS* | Mission Partner Environment-Information System |
| MPE ESC | Mission Partner Environment Executive Steering Committee |
| NRID | Net-Enabled Requirement Identification Database |
| RCDWG | Requirements and Capabilities Development Working Group |
| REL/DMZ* | Releasable Demilitarized Zone |
| UISS* | Unclassified Information Sharing Service |
| US BICES* | United States Battlefield Information Collection and Exploitation System |
| US BICES-X* | United States Battlefield Information Collection and Exploitation System - Extended |
| VDC* | Virtual Data Center |

INTENTIONALLY BLANK

PART II-DEFINITIONS

1. Combined Communications Electronics Board. A five-nation joint military communications-electronics (C-E) organization whose mission is the coordination of any military C-E matter that is referred to it by a member nation. The CCEB member nations are Australia, Canada, New Zealand, the United Kingdom, and the United States. The CCEB Board consists of a senior C4 representative from each member nation.

2. Combined Enterprise Regional Information Exchange System (CENTRIXS). CENTRIXS is a common set of networks built on a set of standard hardware, software, and services for U.S. and Coalition partner forces to share classified operational and intelligence information at the SECRET//REL level. Each of these CENTRIXS networks operates at a single security classification level and operates globally, regionally, and locally.

3. Combined Federated Battle Laboratories Network (CFBLNet). Provides the infrastructure of choice for research, development, trials, and assessments that enables CFBLNet Mission Partners to field, validate, and exercise comprehensive Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance capabilities.

4. Cross Domain Enterprise Service (CDES). Provides support to CCMD, Services, and agencies by implementing, fielding, and providing lifecycle support for cross domain solution technologies that provide secure interoperable capabilities throughout the Department. DISA provides consolidated cross domain solutions on behalf of the DoD components and develops a robust cross domain fielding capability. This is possible by providing net-centric, service-oriented, cross domain information sharing solutions with guaranteed quality of service for authorized users anywhere on the DODIN.

5. Coalition Interoperability Assurance and Validation (CIAV). CIAV is to assure and validate services, systems, and business processes of mission threads that support coalition operations. CIAV improves overall interoperability through the implementation and execution of a coalition-focused, mission-based interoperability methodology enabling multiple nations to fight more efficiently and effectively.

6. Common Mission Network Transport. Enterprise backbone infrastructure that will allow CCMD, Services, and agencies to exchange and share information across regional operational network domains via the Defense Information System Network (DISN) backbone architecture without tunneling

through layers of various transport. CMNT will provide a common transport for encrypted CENTRIXS and encrypted mission partner enclaves traffic to meet mission partner information sharing requirements.

7. Defense Information Systems Agency. A Combat Support Agency that provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint Warfighters, national level leaders, and other mission and Coalition partners across the full spectrum of operations.

8. Department of Defense Information Networks. The globally interconnected, end-to-end set of information capabilities, associated process and personnel for collecting, processing, storing, disseminating, and managing information on demand to Warfighters, policy makers, and support personnel. The DODIN includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems.

9. Enterprise Network. As designated by the DoD CIO Executive Board, a network that provides a defined capability; is available to serve multiple DoD components; complies with the DODIN architecture; is managed with Enterprise-wide oversight; and provides service to any user with a validated requirement.

10. Functional Capabilities Board. FCBs are established bodies that are part of the Joint Capabilities Integration and Development System. They are responsible for the organization, analysis, and prioritization of joint Warfighting capabilities within an assigned functional area.

11. Joint Information Environment. A framework to synchronize and integrate C4ISR capabilities and services delivered through a shared, secure DODIN using standardized guidance designed to achieve the decisive information advantage for the Warfighter. It is comprised of shared information technology infrastructure, enterprise services, and DoD Cybersecurity reference Architecture to achieve full spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies.

12. Mission Partner. Those with which the Department cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments; allies, coalition members, host nations, and other nations; multinational organizations; non-governmental organizations; and the private sector.

13. Mission Partner Environment. A mission partner operating environment that leverages U.S. and mission partner information technology infrastructures with integrating capabilities to realize the DoD JIE framework.

14. Mission Partner Environment Information System. MPE-IS is a DISA-managed modernization effort that enables multinational operations. The DISA IT infrastructure that enables MPE-IS includes networks, cybersecurity, data centers, cross domain solutions, and user interfaces.

15. Pegasus. A CCEB-managed program to interconnect the FVEYs national defense networks to deliver a secure, trusted information sharing environment that supports Defense Cooperation, C2, and the planning and conduct of operations. The Pegasus Program is to deliver selected information sharing services to improve near-real-time collaboration and facilitate access to and the sharing of critical data to enable richer C2 capabilities leveraging existing national applications and infrastructure to the maximum extent possible.

16. SIPR REL DMZ. The primary objective of the SIPR REL network is to provide a consistent, sustainable, secure environment to share real-time, mission-valued information through reliable and controlled access to SIPRNET websites to authorized Coalition partners while maintaining the security and integrity of the SIPRNET. The overall SIPR REL network provides several services that enable information sharing between U.S. SIPRNET users and foreign national/exchange officers embedded in U.S. enclaves and in enclaves located in partner countries.

17. Unclassified Information Sharing Services. The UISS enterprise solution provides unclassified collaboration and information sharing for U.S. Department of Defense and mission partners participating in joint/combined operations, humanitarian assistance and disaster recovery operations, and international conferences or other collaboration events. UISS provides compatible open source software, Commercial Off-the-Shelf Software, and government unique software (e.g., APAN).

18. United States Battlefield Information Collection and Exploitation System. A system that provides NATO forces and other national allied military organizations with near-real-time, correlated, situation and Order Of Battle information supporting threat analysis, targeting, and indications and warning.

19. United States Battlefield Information Collection and Exploitation System – Extended. The primary resource for the dissemination of intelligence data between the U.S. Intelligence Community, CCMDs, the Department, U.S. government services and agencies, and mission partners.

20. Virtual Data Center (VDC). VDC is a modernization of CENTRIXS that supports the MPE-IS reference architecture. The VDC replaces DISA-managed CENTRIXS enclaves and infrastructure to provide MPE-IS global service delivery nodes capable of hosting multiple mission enclaves in support of enduring and episodic missions.

INTENTIONALLY BLANK